The Logical Strength of Büchi's Decidability Theorem

Leszek Aleksander Kołodziejczyk*[1], Henryk Michalewski†[2], Pierre Pradic‡[3], and Michał Skrzypczak§[4]

1 **University of Warsaw, Institute of Mathematics, Warsaw, Poland**
l.kolodziejczyk@mimuw.edu.pl
2 **University of Warsaw, Institute of Mathematics, Warsaw, Poland**
h.michalewski@mimuw.edu.pl
3 **ENS Lyon, Lyon, France**
pierre.pradic@ens-lyon.fr
4 **University of Warsaw, Institute of Informatics, Warsaw, Poland**
m.skrzypczak@mimuw.edu.pl

Abstract

We study the strength of axioms needed to prove various results related to automata on infinite words and Büchi's theorem on the decidability of the MSO theory of $(\mathbb{N}, \leq)$. We prove that the following are equivalent over the weak second-order arithmetic theory RCA_0:

1. Büchi's complementation theorem for nondeterministic automata on infinite words,
2. the decidability of the depth-n fragment of the MSO theory of $(\mathbb{N}, \leq)$, for each $n \geq 5$,
3. the induction scheme for Σ^0_2 formulae of arithmetic.

Moreover, each of (1)–(3) is equivalent to the additive version of Ramsey's Theorem for pairs, often used in proofs of (1); each of (1)-(3) implies McNaughton's determinisation theorem for automata on infinite words; and each of (1)-(3) implies the "bounded-width" version of König's Lemma, often used in proofs of McNaughton's theorem.

1998 ACM Subject Classification F.4.3 Formal Languages

Keywords and phrases nondeterministic automata, monadic second-order logic, Büchi's theorem, additive Ramsey's theorem, reverse mathematics

Digital Object Identifier 10.4230/LIPIcs.CSL.2016.36

1 Introduction

Büchi's theorem [3] states that the monadic second-order theory of $(\mathbb{N}, \leq)$ is decidable. This is one of the fundamental results on the decidability of logical theories, and no less fundamental are the methods developed in order to prove it.

Typical proofs of Büchi's theorem make use of automata on infinite words. Büchi's original argument involved obtaining a complementation theorem for nondeterministic word automata: for each such automaton $\mathcal{A}$, there is another automaton $\mathcal{B}$ which accepts a given word exactly if $\mathcal{A}$ does not. Thanks to the complementation theorem, an MSO formula can be inductively translated into an equivalent nondeterministic automaton. At that point,

* Partially supported by Polish National Science Centre grant no. 2013/09/B/ST1/04390.
† Partially supported by Polish National Science Centre grant no. 2014-13/B/ST6/03595.
‡ Partially supported by Polish National Science Centre grant no. 2014-13/B/ST6/03595.
§ Partially supported by Polish National Science Centre grant no. 2014-13/B/ST6/03595.

25th EACSL Annual Conference on Computer Science Logic (CSL 2016).
Editors: Jean-Marc Talbot and Laurent Regnier; Article No. 36; pp. 36:1–36:16
Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

checking satisfiability of the formula becomes a matter of elementary combinatorics. Another approach to decidability of MSO was presented by Shelah in [16]. Shelah's "composition method" is automata-free, but is similar to Büchi's proof in one important respect: both use a restricted form of Ramsey's Theorem.

McNaughton [12] showed that an infinite word automaton can be determinised, though at the cost of allowing automata with a more general acceptance condition than Büchi's. Since deterministic automata are easy to complement, this again gives the translation of formulae to automata and thus decidability of MSO. To the best of our knowledge all determinisation proofs known from the literature rely on either a restricted form of Ramsey's Theorem or a restricted form of König's Lemma.

It is natural to ask how the various proofs of Büchi's theorem and related results compare to one another. For instance, is determinisation of word automata an "essentially stronger" result than complementation? Also, is the use of mildly nonconstructive principles à la Ramsey or König unavoidable?

A convenient framework for studying questions of this sort is provided by the programme of *reverse mathematics* [17]. The idea is to compare various theorems as formalised in the very expressive language of an axiomatic theory known as *second-order arithmetic*. Typical subtheories of second-order arithmetic are axiomatised by principles asserting the existence of more or less complicated sets of natural numbers. An important example is the relatively weak theory RCA_0, which guarantees only the existence of decidable sets. RCA_0 can formalise a significant amount of everyday mathematics and prove the termination of any primitive recursive algorithm, but it is unable to prove the existence of noncomputable objects such as the homogeneous sets postulated by Ramsey's Theorem or the infinite branches postulated by König's Lemma. Sometimes it is possible to show that two theorems not provable in RCA_0 are provably equivalent in it, and thus neither theorem is logically stronger than the other in the sense of requiring more abstract or less constructive sets. It is also often the case that a set existence principle used to derive some theorem is actually implied by the theorem over RCA_0. This serves as evidence that the principle is in fact necessary to prove the theorem.

In this paper, we carry out a reverse-mathematical study of the results around Büchi's theorem. We have two main aims in mind. One is to compare complementation, determinisation and decidability of MSO in terms of logical strength. The other aim is to clarify the role of Ramsey's Theorem and König's Lemma in proofs of Büchi's theorem and the related facts about automata. This seems interesting in light of the fact that the usual formulation of Ramsey's Theorem for pairs and the so-called Weak König's Lemma (the form of König's Lemma most commonly needed in practice) are known to be incomparable over RCA_0 [6, 11].

Our findings are as follows: firstly, determinisation of infinite word automata is no stronger than complementation, at least in the sense of implication over RCA_0. Secondly, decidability of MSO over $(\mathbb{N}, \leq)$ implies both complementation and determinisation. Finally, the use of Ramsey- or König-like principles in proofs of Büchi's theorem is mostly spurious in the sense that the versions that are actually needed follow from a very limited set-existence principle, namely mathematical induction for properties expressed by Σ^0_2 formulae. More precisely, we prove:

▶ **Theorem 1.** *Over* RCA_0*, the following statements are equivalent:*
1. *the principle of mathematical induction for* Σ^0_2 *formulae (denoted* Σ^0_2-IND*),*
2. *the Additive Ramsey Theorem (see Definition 2),*
3. *complementation for Büchi automata: there exists an algorithm which for each nondeterministic Büchi automaton* $\mathcal{A}$ *outputs a Büchi automaton* $\mathcal{B}$ *such that for every infinite word* α*,* $\mathcal{B}$ *accepts* α *exactly if* $\mathcal{A}$ *does not accept* α*,*

4. *the decidability of the depth-n fragment of the MSO theory of* $(\mathbb{N}, \leq)$ *(where* $n \geq 5$ *is a natural number)*[1]*.*

Furthermore, each of 1.–4. implies:

5. *determinisation of Büchi automata: there exists an algorithm which for each nondeterministic Büchi automaton* $\mathcal{A}$ *outputs a deterministic Rabin automaton* $\mathcal{B}$ *such that for every infinite word* α*,* $\mathcal{B}$ *accepts* α *exactly if* $\mathcal{A}$ *accepts* α*.*

We also give a precise statement of the bounded-width form of König's Lemma often used in proofs of Item 5., and show that it is implied by each of 1.–4. Interestingly, it is not clear if 5. implies 1.–4. over RCA_0: standard arguments used to complement deterministic automata with acceptance conditions other than Büchi seem to involve Σ^0_2-IND.

It follows from our results that Büchi's theorem is unprovable in RCA_0, but only barely: it is true in computable mathematics, in the sense that the theorem remains valid if all the set quantifiers are restricted to range over (exactly) the decidable subsets of $\mathbb{N}$. This is in stark contrast to the behaviour of Rabin's theorem on the decidability of MSO on the infinite binary tree, which is known to require the existence of extremely complicated noncomputable sets [9]. Also Additive Ramsey's Theorem and Bounded-width König's Lemma are true in computable mathematics—quite unlike more general forms of Ramsey's Theorem for pairs and König's Lemma [7, 10].

To prove the implication $(4 \to 1)$ of Theorem 1, we come up with a family of MSO sentences for which truth in $(\mathbb{N}, \leq)$ is undecidable if Σ^0_2-IND fails. The other implications are proved by formalising more or less standard arguments from automata theory. In some cases this is routine, but especially the proof of $(1 \to 5)$ is quite delicate: we have to check not only that Σ^0_2-IND implies Bounded-width König's Lemma, but also that constructing the objects to which we apply the lemma is within the means of $\mathsf{RCA}_0 + \Sigma^0_2$-$\mathsf{IND}$.

The structure of the paper is as follows. Sections 2 and 3 discuss the necessary background on reverse mathematics, automata, and MSO. We prove $(1 \to 2)$ in Section 4, $(2 \to 3)$ in Section 5, $(3 \to 4)$ in Section 6, $(4 \to 1)$ in Section 7. Section 8 contains a proof that Σ^0_2-IND implies Bounded-width König's Lemma, which is then applied to prove $(1 \to 5)$ in Section 9.

2 Background on reverse mathematics

Reverse mathematics [17] is a framework for studying the strength of axioms needed to prove theorems of countable mathematics, that is, the part of mathematics concerned with objects that can be represented using no more than countably many bits of information. This encompasses the vast majority of the mathematics needed in computer science.

The basic idea of reverse mathematics is to analyse mathematical theorems in terms of subsystems of a strong axiomatic theory known as second-order arithmetic. The two-sorted language of second-order arithmetic, L_2, contains *first-order* variables $x, y, z, \ldots$ (or $i, j, k, \ldots$), intended to range over natural numbers, and *second-order* variables $X, Y, Z, \ldots$, intended to range over sets of natural numbers. L_2 includes the usual arithmetic functions and relations $+, \cdot, \leq, 0, 1$ on the first-order sort, and the $\in$ relation which has one first-order and one second-order argument. The intended model of Z_2 is $(\omega, \mathcal{P}(\omega))$.

Notational convention. From this point onwards, we will use the letter $\mathbb{N}$ to denote the natural numbers as formalised in second-order arithmetic, that is, the domain of the first-

[1] The restriction to fixed-depth fragments is a technicality related to undefinability of truth. This is explained in more detail in Section 3.

order sort. On the other hand, the symbol ω will stand for the concrete, or standard, natural numbers. For instance, given a theory T and a formula $\varphi(x)$, "T proves $\varphi(n)$ for all $n \in \omega$" will mean "$\mathrm{T} \vdash \varphi(0), \mathrm{T} \vdash \varphi(1), \ldots$", which does not have to imply $\mathrm{T} \vdash \forall x \in \mathbb{N}.\, \varphi(x)$.

Full second-order arithmetic, Z_2, has axioms of three types: (i) axioms stating that the first-order sort is the non-negative part of a discretely ordered ring; (ii) comprehension axioms, or sentences of the form

$$\forall \bar{Y}\, \forall \bar{y}\, \exists X\, \forall x \left(x \in X \Leftrightarrow \varphi(x, \bar{Y}, \bar{y})\right),$$

where φ is an arbitrary formula of L_2 not containing the variable X; (iii) the induction axiom,

$$\forall X \left[0 \in X \wedge \forall x\, (x \in X \Rightarrow x+1 \in X) \Rightarrow \forall x.\ x \in X\right].$$

The language L_2 is very expressive, as the first-order sort can be used to encode arbitrary finite objects and the second-order sort can encode even such objects as complete separable metric spaces, continuous functions between them, and Borel sets within them (cf. [17, Chapters II.5, II.6, and V.3]). Moreover, the theory Z_2 is powerful enough to prove almost all theorems from a typical undergraduate course that are expressible in L_2. In fact, the basic observation underlying reverse mathematics [17] is that many important theorems are equivalent to various fragments of Z_2, where the equivalence is proved in some specific weaker fragment, referred to as the *base theory*.

Quantifier hierarchies. Typical fragments of Z_2 are defined in terms of well-known quantifier hierarchies whose definitions we now recall. A formula is Σ^0_n if it has the form $\exists \bar{x}_1\, \forall \bar{x}_2\, \ldots\, \mathsf{Q}\bar{x}_n.\ \psi$, where the $\bar{x}_i$'s are blocks of first-order variables, the shape of Q depends on the parity of n, and ψ is Δ^0_0, i.e. contains only bounded first-order quantifiers. A formula is Π^0_n if it is the negation of a Σ^0_n formula. A formula is *arithmetical* if it contains only first-order quantifiers (second-order parameters are allowed).

A formula is Σ^1_n if it has the form $\exists \bar{X}_1\, \forall \bar{X}_2\, \ldots \mathsf{Q}\bar{X}_n.\ \psi$, where the $\bar{X}_i$'s are blocks of first-order variables, the shape of Q depends on the parity of n, and ψ is arithmetical. A formula is Π^1_n if it is the negation of a Σ^1_n formula.

In practice, we say that a formula is Σ^i_n/Π^i_n if it equivalent to a Σ^i_n/Π^i_n formula in the axiomatic theory we are working in at a given point.

Definition of $\mathsf{RCA_0}$. The usual base theory in reverse mathematics is RCA_0, which guarantees only the existence of decidable sets. RCA_0 is defined by restricting the comprehension scheme to Δ^0_1-comprehension, which takes the form:

$$\forall \bar{Y}\, \forall \bar{y}\, \left[\forall x\, (\varphi(x, \bar{Y}, \bar{y}) \Leftrightarrow \neg\psi(x, \bar{Y}, \bar{y})) \Rightarrow \exists X\, \forall x\, (x \in X \Leftrightarrow \varphi(x, \bar{Y}, \bar{y}))\right],$$

where both φ and ψ are Σ^0_1. For technical reasons, it is necessary to strengthen the induction axiom to Σ^0_1-IND, that is, the scheme Σ^0_1-IND consisting of the sentences

$$\forall \bar{Y}\, \forall \bar{y}\, \left[\varphi(0, \bar{Y}, \bar{y}) \wedge \forall x\, \left(\varphi(x, \bar{Y}, \bar{y}) \Rightarrow \varphi(x+1, \bar{Y}, \bar{y})\right) \Rightarrow \forall x.\ \varphi(x, \bar{Y}, \bar{y})\right]$$

for φ in Σ^0_1. Σ^0_1-IND makes it possible to define sequences by primitive recursion (cf. [17, Theorem II.3.4]): given some x_0 and a function $f\colon \mathbb{N} \to \mathbb{N}$, RCA_0 proves that there is a unique sequence $(x_i)_{i \in \mathbb{N}}$ such that $x_{i+1} = f(x_i)$ for each i.

RCA_0 has a unique minimal model in the sense of embeddability. This minimal model is (ω, Dec), where Dec is the family of decidable subsets of ω.

The Σ^0_n-IND scheme. In this paper we study an extension of RCA_0 obtained by strengthening the induction scheme to Σ^0_2 formulae. In general, for $n \in \omega$, the axiom scheme Σ^0_n-IND is defined just like Σ^0_1-IND, but with the induction formula φ in Σ^0_n rather than Σ^0_1. For each n, $\mathsf{RCA}_0 + \Sigma^0_n$-IND is equivalent to $\mathsf{RCA}_0 + \Pi^0_n$-IND, where the latter is defined in the natural way, as well as to the least number principle for Σ^0_n or Π^0_n formulae (cf. [17, Chapter II.3]).

Two important principles provable from Σ^0_n-IND are Σ^0_n-*collection*:

$$\forall \bar{Z}\, \forall \bar{z} \left[\forall x \leq t\, \exists y.\ \varphi(x, y, \bar{Z}, \bar{z})\right] \Rightarrow \exists w\, \forall x \leq t\, \exists y \leq w.\ \varphi(x, y, \bar{Z}, \bar{z}),$$

for φ in Σ^0_n, and *bounded* Σ^0_n-*comprehension*:

$$\forall \bar{Y}\, \forall \bar{y}\, \forall w\, \exists X\, \forall x\, (x \in X \Leftrightarrow x \leq w \wedge \varphi(x, \bar{Y}, \bar{y})),$$

for φ in Σ^0_n.

For each n, the theory $\mathsf{RCA}_0 + \Sigma^0_{n+1}$-IND is strictly stronger than $\mathsf{RCA}_0 + \Sigma^0_n$-IND (cf. e.g. [4, Theorem IV.1.29]). However, note that the minimal model (ω, Dec) of RCA_0 satisfies $\mathsf{RCA}_0 + \Sigma^0_n$-IND for all n, because an induction axiom is always true in a model with first-order universe ω.

Additive Ramsey's Theorem and Bounded-width König's Lemma. Two prominent extensions of RCA_0 are related to weak forms of important nonconstructive set existence principles: König's Lemma and Ramsey's Theorem.

Weak König's Lemma is the statement: "for every k, every infinite tree contained in $\{0, 1, \ldots, k\}^*$ has an infinite branch". The theory obtained by adding this statement to RCA_0 is known as WKL_0. This is the minimal theory supporting all sorts of "compactness arguments" in combinatorics, topology, analysis, and elsewhere (cf. [17, Chapter IV]).

The theory RT^2_2 extends RCA_0 by an axiom expressing Ramsey's Theorem for pairs and two colours[2]: for every 2-colouring of $[\mathbb{N}]^2$ there exists an infinite homogeneous set. $\mathsf{RT}^2_{<\infty}$ is defined similarly but allowing k-colourings for each $k \in \mathbb{N}$.

Both RT^2_2 and $\mathsf{RT}^2_{<\infty}$ are known to be incomparable with WKL_0 in the sense of implication over RCA_0 [6, 11]. WKL_0, RT^2_2, and RT^2_∞ are all false in the minimal model (ω, Dec) of RCA_0 [7, 10]. Much more on these theories can be found in [5].

In this paper, we study specific restricted versions of WKL_0 and $\mathsf{RT}^2_{<\infty}$ which play a role in proofs of Büchi's theorem. Recall that a *semigroup* is a set S with an associative operation $*\colon S \times S \to S$.

▶ **Definition 2** (Additive Ramsey Theorem). The *Additive Ramsey Theorem* is the following statement: for every finite semigroup $(S, *)$ and every colouring $C\colon [\mathbb{N}]^2 \to S$ such that for every $i < j < k$ we have $C(i, j) * C(j, k) = C(i, k)$, there exists an infinite homogeneous set $I \subseteq \mathbb{N}$. That is, there is a fixed color a such that for every $(i, j) \in [I]^2$, $C(i, j) = a$.

▶ **Definition 3** (Bounded-width König's Lemma). *Bounded-width König's Lemma* is the following statement: for every finite set Q and every graph G whose vertices belong to $Q \times \mathbb{N}$ and whose edges are all of the form $((q, i), (q', i+1))$ for some $q, q' \in Q$, if there are arbitrarily long finite paths in G starting in some vertex $(q, 0)$, then there is an infinite path in G starting in $(q, 0)$.

[2] By $[X]^2$ we denote the set of unordered pairs of elements of X.

Notice that Bounded-width König's Lemma applied to a graph G is essentially the same as Weak König's Lemma applied to the tree obtained by the so-called unraveling of G (in particular, Bounded-width König's Lemma is provable in WKL_0). However, the graph formulation is more natural to express.

3 Background on MSO and Büchi automata

Büchi automata and MSO logic are equivalent formalisms for specifying properties of infinite words. In this section we formally introduce these concepts. If not stated otherwise, the formalisation presented here is carried out in RCA_0.

Infinite words. By Σ we denote a finite nonempty set called an *alphabet*. A *finite word* over Σ is a function $w\colon \{0,\dots,k-1\} \to \Sigma$; the *length* of w is k. The set of all finite words over Σ is denoted Σ^*. An *infinite word* over Σ is a function $\alpha\colon \mathbb{N} \to \Sigma$. We write $\alpha \in \Sigma^{\mathbb{N}}$ for "α is an infinite word over Σ".

Every infinite word can be treated as a relational structure with the universe $\mathbb{N}$ and predicates: the binary order predicate $\leq$ and a unary predicate a for every $a \in \Sigma$. The semantics of these predicates over a given infinite word α is natural, in particular $a(x)$ holds if $\alpha(x) = a$.

When working with automata and logic it is customary to define *languages*—sets of infinite words satisfying certain properties. However, from the point of view of second-order arithmetic a language is a "third-order object". Therefore, in this paper we avoid talking directly about languages. Instead, when we want to express some properties of languages, we explicitly quantify over infinite words with a given property.

Automata over infinite words. A (nondeterministic) Büchi automaton is a tuple $\mathcal{A} = \langle Q, \Sigma, q_{\mathrm{I}}, \delta, F\rangle$ where: Q is a finite set of *states*, Σ is an alphabet, $q_{\mathrm{I}} \in Q$ is an *initial state*, $\delta \subseteq Q \times \Sigma \times Q$ is the *transition relation*, and $F \subseteq Q$ is the set of *accepting states*. Given an infinite word $\alpha \in \Sigma^{\mathbb{N}}$, we say that $\rho \in Q^{\mathbb{N}}$ is a *run* of $\mathcal{A}$ over α if $\rho(0) = q_{\mathrm{I}}$ and for every $n \in \mathbb{N}$ we have $\big(\rho(n), \alpha(n), \rho(n+1)\big) \in \delta$. A run ρ is *accepting* if $\rho(n) \in F$ for infinitely many $n \in \mathbb{N}$. An automaton $\mathcal{A}$ *accepts* α if there exists an accepting run of $\mathcal{A}$ over α. An automaton is *deterministic* if for every $q \in Q$ and $a \in \Sigma$ there is at most one transition of the form $(q, a, q') \in \delta$. When the automaton is not clear from the context, we put it in the superscript, i.e. $Q^{\mathcal{A}}$ is the set of states of $\mathcal{A}$.

The possible transitions of a Büchi automaton over a particular letter $a \in \Sigma$ can be encoded as a *transition matrix* $M_a\colon Q \times Q \to \{0, 1, \star\}$, where $M_a(q, q') = 0$ if $(q, a, q') \notin \delta$, otherwise $M_a(q, q') = \star$ if $q \in F$, and otherwise $M_a(q, q') = 1$. Let $[Q]$ be the set of all such functions $M\colon Q \times Q \to \{0, 1, \star\}$.

Since deterministic Büchi automata are strictly weaker than general Büchi automata [14], one introduces the more flexible *Rabin acceptance condition* in order to determinise Büchi automata. A *Rabin automaton* is a tuple $\mathcal{A} = \langle Q, \Sigma, q_{\mathrm{I}}, \delta, (E_i, F_i)_{i=1}^{k}\rangle$ as in the case of Büchi automata, where $E_i, F_i \subseteq Q$ for $i = 1, \dots, k$. A run $\rho \in Q^{\mathbb{N}}$ of $\mathcal{A}$ is *accepting* if and only if for some $i \in \{1, \dots, k\}$ each state in E_i appears only finitely many times in ρ and some state in F_i appears infinitely many times in ρ.

In general (i.e. in Z_2) Rabin automata can easily be complemented into so-called *Streett automata*, and both classes can be transformed into nondeterministic Büchi automata. However, the transformations into Büchi automata require more than RCA_0. For Streett automata, Σ^0_2-IND seems necessary. For Rabin, we need the Büchi automaton to guess that no state from a given set of states will reappear in the run under consideration. To prove that such a construction is correct one needs Σ^0_2-collection—within RCA_0 the fact that in a given run ρ each state $q \in E$ appears only finitely many times does not imply a global bound after which no state from E reappears. That is the essential reason why it is not clear whether Item 5. of Theorem 1 implies the other items in RCA_0.

Monadic Second-Order logic. Monadic second-order logic (MSO) is an extension of first-order logic. MSO logic allows: boolean connectives $\neg$, $\vee$, $\wedge$; the first-order quantifiers $\exists x$ and $\forall x$; and the monadic second-order quantifiers $\exists X$ and $\forall X$, where the variable X ranges over subsets of the universe. Apart from predicates from the signature of a given structure, the logic admits the binary predicate $x \in X$ with the natural semantics.

Definition of truth for MSO over $\mathbb{N}$. In order to state our theorems involving decidability of the MSO theory of $(\mathbb{N}, \leq)$, we need to formulate the semantics of monadic second-order logic within RCA_0. This involves a coding of formulae $\phi \mapsto \ulcorner\phi\urcorner$; we identify a formula with its code. However, in second-order arithmetic there is no canonical definition of truth in an infinite structure which would work for all of MSO. Moreover, by Tarski's theorem on the undefinability of truth, for some infinite structures there is no such definition at all. In particular, it is not at all clear how to state the decidability of MSO$(\mathbb{N}, \leq)$ as a single sentence.

On the other hand, already RCA_0 is able to express a truth definition for the *depth-n fragment of MSO*, for each $n \in \omega$. Here the depth of a formula is calculated as the largest number of alternating blocks of $\wedge/\forall$'s and $\vee/\exists$'s appearing on a branch in the syntactic tree of the formula (assume that all negations are pushed inside using the De Morgan laws). Essentially, the truth definition needs one universal set quantifier for a block of $\wedge/\forall$'s and one existential set quantifier for a block of $\vee/\exists$'s[3].

So, what is possible is to provide formulae φ_n stating that the depth-n fragment of MSO$(\mathbb{N}, \leq)$ is decidable. We show in Section 6 that every φ_n can be proved in RCA_0 assuming a complementation procedure for Büchi automata, and in Section 7 that φ_5 implies Σ^0_2-IND. As a corollary, we can observe that $\mathsf{RCA}_0 \vdash \varphi_5 \Rightarrow \varphi_n$ for every $n \in \omega$.

The Büchi decidability theorem. In [3] Büchi proved decidability of the theory MSO$(\mathbb{N}, \leq)$. The following theorem captures as much of Büchi's result as can be naturally expressed in relatively weak theories of second-order arithmetic.

▶ **Theorem 4** (Büchi formalised). *There exists an effective procedure P such that for every fixed depth $n \in \omega$ the following is provable in $\mathsf{RCA}_0 + \Sigma^0_2$-$\mathsf{IND}$. For every statement ϕ of MSO over an alphabet Σ such that the depth of ϕ is at most n, the procedure $P(\phi)$ produces a nondeterministic Büchi automaton $\mathcal{A}$ over Σ such that for every infinite word $\alpha \in \Sigma^{\mathbb{N}}$, this word satisfies ϕ if and only if $\mathcal{A}$ accepts α. Moreover, it is decidable if a given nondeterministic Büchi automaton accepts any infinite word.*

We discuss some issues related to formalising the inductive proof of Büchi's theorem in Section 6. The crucial step concerns complementation of automata, which is used to treat negations of subformulae in ϕ (or subformulae beginning with $\forall$, assuming the negations have been pushed inside).

[3] After slight modifications, the truth definition would still work if we allowed depth-n formulas to contain arbitrarily many alternations $\wedge$'s and $\vee$'s inside the scope of the last quantifier counted towards the depth.

4 Σ^0_2-IND implies Additive Ramsey

The aim of this section is to prove the following theorem.

▶ **Theorem 5.** *Over* RCA_0, Σ^0_2-IND *implies Additive Ramsey's Theorem (see Definition 2).*

The proof consists of two steps. First, we prove another weakening of Ramsey's Theorem.

▶ **Definition 6.** *Ordered Ramsey's Theorem* for pairs states that if $(P, \preceq)$ is a finite partial order and $C\colon [\mathbb{N}]^2 \to P$ is a colouring such that for every $i < j < k$ we have $C(i,j) \succeq C(i,k)$, then there exists an infinite homogeneous set $I \subseteq \mathbb{N}$, i.e. $C(i,j) = C(i',j')$ for all $(i,j),(i',j') \in [I]^2$.

Note that this statement follows immediately from the so-called *Stable Ramsey's Theorem* $\mathsf{SRT}^2_{<\infty}$ (cf. [5, Sections 6.4 and 6.8]), where the requirement on C is only that $C(i,\cdot)$ should stabilise for each i.

▶ **Lemma 7.** *Over* RCA_0, Σ^0_2-IND *proves Ordered Ramsey's Theorem.*

Proof. We call a colour $p \in P$ *recurring* if $\forall i\, \exists k > j > i.\ C(j,k) = p$. Notice that for each non-recurring colour p there exists i_p such that there is no occurrence of p to the right of i_p (i.e. no $k > j > i_p$ such that $C(j,k) = p$). By an application of Σ^0_2-collection we obtain some i_0 such that for every non-recurring colour p and every $k > j > i_0$ we have $C(j,k) \neq p$. In particular, there is a recurring colour. Moreover, being a recurring colour is a Π^0_2 property, so by Σ^0_2-IND we can find a $\preceq$-minimal recurring colour p_0.

We now define a sequence $(u_i, v_i)_{i\in\mathbb{N}}$ by primitive recursion on i. Let (u_0, v_0) be some pair such that $i_0 < u_0 < v_0$ and $c(u_0, v_0) = p_0$. Now assume that $u_0 < v_0 \leq u_1 < v_1 \ldots \leq u_i < v_i$ have been defined, $\{u_0, \ldots, u_i\}$ is homogeneous with colour p_0, and $C(u_i, v_i) = p_0$. Let (u_{i+1}, v_{i+1}) be the smallest pair such $v_i \leq u_{i+1} < v_{i+1}$ and $C(u_{i+1}, v_{i+1}) = p_0$. Such a pair exists because p_0 is recurring. We know that $C(u_i, u_{i+1}) = p_0$, since on the one hand $C(u_i, u_{i+1}) \preceq C(u_i, v_i) = p_0$, and on the other hand $u_i > i_0$ and thus $C(u_i, u_{i+1})$ is a recurring colour, so it cannot be $\preceq$-strictly smaller than p_0. Similarly, for $j < i$ we know that $C(u_j, u_{i+1}) = p_0$ because $C(u_j, u_{i+1}) \preceq p_0$ and $u_j > i_0$. Therefore, the set $\{u_i \mid i \in \mathbb{N}\}$ is homogeneous for C. ◀

Before proceeding to prove the additive version of the theorem, we recall a few basic facts about finite semigroups we shall use in our proof. The facts are proved by elementary combinatorial arguments which readily formalise in RCA_0. The proofs can be found for instance in [14].

▶ **Definition 8.** Green preorders over a semigroup S are defined as follows

- $s \leq_{\mathcal{R}} t$ if and only if $s = t$ or $s \in t * S = \{t * a \mid a \in S\}$,
- $s \leq_{\mathcal{L}} t$ if and only if $s = t$ or $s \in S * t = \{a * t \mid a \in S\}$,
- $s \leq_{\mathcal{H}} t$ if and only if $s \leq_{\mathcal{R}} t$, and $s \leq_{\mathcal{L}} t$.

The associated equivalence relations are written $\mathcal{R}$, $\mathcal{L}$, $\mathcal{H}$; their equivalence classes are called respectively $\mathcal{R}$, $\mathcal{L}$, and $\mathcal{H}$-classes.

▶ **Lemma 9.** *For every finite semigroup S and $s,t \in S$, $s \leq_{\mathcal{L}} t$ and $s\ \mathcal{R}\ t$ implies $s\ \mathcal{H}\ t$.*

▶ **Lemma 10** ([14, Proposition 2.4]). *If $(S,*)$ is a finite semigroup, $H \subseteq S$ an $\mathcal{H}$-class, and some $a, b \in H$ satisfy $a * b \in H$ then for some $e \in H$ we know that $(H, *, e)$ is a group.*

Now we can prove our main statement.

Proof of Theorem 5. Let a colouring C take values in the finite semigroup $(S, *)$ and satisfy the additivity condition of Definition 2. For every position i and every $k \geq j > i$, let us observe that $C(i,k) \leq_{\mathcal{R}} C(i,j)$. Let r be the function mapping every element of S to its $\mathcal{R}$-class. The function $r \circ C$ is an ordered colouring; let us use Lemma 7 to obtain a homogeneous sequence $(u_i)_{i \in \mathbb{N}}$ for $r \circ C$.

Since S is finite, we can use Σ^0_2-collection to prove that there is some colour a such that $C(u_0, u_i) = a$ for infinitely many i. This lets us take a subsequence $(v_i)_{i \geq 0}$ of $(u_i)_{i \geq 0}$ such that $C(v_0, v_i) = a$ for each i.

We now know that $a = a * C(v_i, v_j)$ for every $0 < i < j$. In particular, $a \leq_{\mathcal{L}} C(v_i, v_j)$ by the definition of $\leq_{\mathcal{L}}$. Since a and $C(v_i, v_j)$ are $\mathcal{R}$-equivalent, Lemma 9 implies that $C(v_i, v_j)\ \mathcal{H}\ a$. Let H be the $\mathcal{H}$-class of a. Since $a * C(v_i, v_j) = a \in H$ we know by Lemma 10 that $(H, *, e)$ is a group for some $e \in H$. Using this group structure and the equation $a = a * C(v_i, v_j)$ we obtain that $C(v_i, v_j) = e$. Hence, $\{v_{i+1} \mid i \in \mathbb{N}\}$ is a homogeneous set for C with the colour e. ◀

We will now sketch the opposite implication, as stated by the following lemma. It follows from the other implications of Theorem 1, thus the reasoning presented here is not needed to obtain the theorem. However, we decided to include it, as the argument is very straightforward and avoids the use of automata and logic.

▶ **Lemma 11.** *Over* RCA_0*, Additive Ramsey's Theorem implies* Σ^0_2-IND.

Proof sketch. By the construction from Section 7, a failure of Σ^0_2-IND gives us $a \in \mathbb{N}$ and an infinite word $\alpha \in \{0, \ldots, a+1\}^{\mathbb{N}}$ such that there is no highest letter i that appears infinitely many times in α. Fix such a word α and consider the colouring with values in $\{0, \ldots, a+1\}$ defined for $i < j$ as follows:

$$C(i,j) = \max\{\alpha(k) \mid i \leq k < j\}.$$

Clearly, C is an additive colouring of $[\mathbb{N}]^2$ by elements of the semigroup $(\{0, \ldots, a+1\}, \max)$. Apply Additive Ramsey's Theorem to obtain an infinite homogeneous set $I \subseteq \mathbb{N}$ for C. Assume that $i \in \{0, \ldots, a+1\}$ is the colour of I. By the definition of C, i is the highest colour that appears infinitely many times in α. ◀

In the full version of the paper, we additionally provide a direct proof that Ordered Ramsey's Theorem implies Σ^0_2-IND.

5 Additive Ramsey implies complementation

In this section, we sketch a proof of the following theorem.

▶ **Theorem 12.** *Over* RCA_0*, the Additive Ramsey Theorem (see Definition 2) implies the following complementation result: there exists an algorithm which, given a Büchi automaton* $\mathcal{A}$ *over an alphabet* Σ*, outputs a Büchi automaton* $\mathcal{B}$ *over the same alphabet such that for every* $\alpha \in \Sigma^{\mathbb{N}}$ *we have that* $\mathcal{A}$ *accepts* α *if and only if* $\mathcal{B}$ *does not accept* α.

The proof of this theorem follows the standard construction of the automaton $\mathcal{B}$ [3]: the states of $\mathcal{B}$ are based on transition matrices of $\mathcal{A}$ (see Section 3). The automaton $\mathcal{B}$ guesses a Ramseyan decomposition of the given infinite word α with respect to a certain homomorphism into $[Q]$; and then verifies that the decomposition witnesses that there cannot be any accepting run of $\mathcal{A}$ over α. A complete proof of the theorem will be given in the full version of the paper.

6 Complementation implies decidability

▶ **Theorem 13.** *For any $n \in \omega$, the following is provable in* RCA_0*: if there exists an algorithm for complementing Büchi automata, then there exists an algorithm which, given an MSO formula ϕ of depth at most n, outputs an automaton $\mathcal{A}_\phi$ such that for every word ν, ν satisfies the formula ϕ if and only if ν is accepted by $\mathcal{A}_\phi$. As a consequence, the depth-n fragment of MSO$(\mathbb{N}, \leq)$ is decidable.*

A detailed proof of the theorem will be given in the full version of the paper. Te argument is along the lines of the standard inductive construction of an automaton $\mathcal{A}_\phi$ that simulates the behaviour of ϕ. Let us recall that in RCA_0 we only have truth definitions for fixed-depth MSO formulae. Additionally, each such truth definition is not a Σ^0_1 formula (it is not even arithmetical, as it quantifies over infinite words). Therefore, in RCA_0 we cannot perform any induction involving the truth definition. This fact has two consequences:

1. in the above theorem, the implication from complementation to decidability is stated for all $n \in \omega$ separately and its proof is obtained via an external induction over n,
2. our construction of $\mathcal{A}_\phi$ needs to work in a fixed number of steps (depending on n), no iterative procedure can be involved. In particular, we need to simulate whole blocks of quantifiers or connectives at once.

To complete the proof of the theorem, we verify in RCA_0 that the emptiness problem is decidable for Büchi automata, as expressed by the following lemma.

▶ **Lemma 14.** *Provably in* RCA_0*, it is decidable if, given a nondeterministic Büchi automaton $\mathcal{A}$, there exists an infinite word accepted by $\mathcal{A}$.*

7 Decidability implies Σ^0_2-IND

In this section we prove the following theorem.

▶ **Theorem 15.** *Over* RCA_0*, the decidability of the depth-5 fragment of MSO$(\mathbb{N}, \leq)$ implies* Σ^0_2-IND.

The rest of this section is devoted to a proof of this theorem. Consider a Π^0_2 formula (with parameters we keep implicit) $\phi(i) \equiv \forall x\, \exists y.\ \delta(i, x, y)$ and suppose it satisfies the premises of induction, i.e. $\phi(0)$ holds and $\forall i\, (\phi(i) \Rightarrow \phi(i+1))$. Take $a \in \mathbb{N}$. We want to show that $\phi(a)$ holds. For that we will use decidability of the depth-5 fragment of MSO$(\mathbb{N}, \leq)$ to prove using Σ^0_1-IND that a certain formula ψ_{a+1} is true in $(\mathbb{N}, \leq)$. We will construct a specific infinite word that encodes the semantics of $\phi(a)$ and use the fact that the word satisfies ψ_{a+1} to deduce that $\phi(a)$ holds.

For $k \in \mathbb{N}$ let ψ_k be the MSO formula stating "for every infinite word over the alphabet $\{0, \dots, k\}$ there is a maximal letter $i \in \{0, \dots, k\}$ occurring infinitely often". More formally, ψ_k is defined as follows.

$$\psi_k \equiv \quad \forall X_0\, \forall X_1 \dots \forall X_k \left[\forall x \left(\bigvee_{i \leq k} x \in X_i \wedge \bigwedge_{i<j\leq k} \neg(x \in X_i \wedge x \in X_j) \right) \Longrightarrow \bigvee_{i \leq k} \left((\forall x\, \exists y \geq x.\ y \in X_i) \wedge \bigwedge_{i<j\leq k} (\exists x\, \forall y \geq x.\ y \notin X_j) \right) \right]. \tag{1}$$

The formula ψ_k is an MSO formula of depth 5. By the assumption on decidability, the property that ψ_k belongs to the theory $\mathrm{MSO}(\mathbb{N}, \leq)$ can be expressed by a Σ^0_1 formula of second-order arithmetic, $\Psi(k)$ (and, in fact, by a Π^0_1 formula as well). Clearly, in RCA_0 we can prove that ψ_0 belongs to $\mathrm{MSO}(\mathbb{N}, \leq)$ and for every $i \in \mathbb{N}$, if ψ_i belongs to $\mathrm{MSO}(\mathbb{N}, \leq)$, then ψ_{i+1} belongs to $\mathrm{MSO}(\mathbb{N}, \leq)$. Therefore, by the assumption on Ψ, we know that $\Psi(0)$ holds and $\forall i\, (\Psi(i) \Rightarrow \Psi(i+1))$. Then, Σ^0_1-IND guarantees that $\Psi(a+1)$ is true and hence ψ_{a+1} belongs to $\mathrm{MSO}(\mathbb{N}, \leq)$.

Now our aim is to construct a specific infinite word α over the alphabet $\{0, \ldots, a+1\}$ in such a way to guarantee that Claim 16 below holds.

For $i \leq a$ and $w \in \mathbb{N}$ let $C(i, w) = \max \big\{v \leq w \mid \forall x < v\, \exists y < w.\ \delta(i, x, y)\big\}$.

Clearly the function $C(i, w)$ is computable. Assume a computable enumeration[4] for pairs $\langle \cdot, \cdot \rangle \colon \mathbb{N}^2 \to \mathbb{N}$ that is monotone with respect to the coordinatewise order on $\mathbb{N}^2$. Define an infinite word

$$\alpha(n) = \begin{cases} i+1 & \text{if } n = \langle i, w \rangle,\ i \leq a, \text{ and } C(i, w) > \big|\{w' < w \mid \alpha(\langle i, w' \rangle) = i+1\}\big|, \\ 0 & \text{otherwise.} \end{cases}$$

Again, $\alpha(n)$ is computable so α can be defined by Δ^0_1-comprehension. We will prove in RCA_0 the following claim.

▶ **Claim 16.** *For every $i \leq a$ and $v \in \mathbb{N}$ the letter $i+1$ appears at least v times in α if and only if $\forall x < v\, \exists y.\ \delta(i, x, y)$. In particular, $i+1$ appears infinitely many times in α if and only if $\phi(i)$ holds.*

Proof. First assume that $\forall x < v\, \exists y.\ \delta(i, x, y)$ holds for some $i \leq a$ and $v \in \mathbb{N}$. By Σ^0_1-collection, there exists some w such that $\forall x < v\, \exists y < w.\ \delta(i, x, y)$. Let $k = \big|\{w' < w \mid \alpha(\langle i, w' \rangle) = i+1\}\big|$. If $k \geq v$ then we are done. Assume the contrary and notice that $C(i, w) \geq v$. This means that for $w' = w, w+1, \ldots, w+v-k-1$ we have $\alpha(\langle i, w' \rangle) = i+1$ (we use Σ^0_1-IND to prove this). In total this gives us v positions of α that are labelled by $i+1$.

Now assume that there are at least v positions of α labelled by $i+1$. Let w_0 be the minimal position such that $\big|\{w' \leq w_0 \mid \alpha(\langle i, w' \rangle) = i+1\}\big| = v$. In particular we know that $\alpha(\langle i, w_0 \rangle) = i+1$ and $\big|\{w' < w_0 \mid \alpha(\langle i, w' \rangle) = i+1\}\big| = v-1$. This means that $C(i, w_0) \geq v$. By the definition of $C(i, w)$, it follows that $\forall x < v\, \exists y.\ \delta(i, x, y)$ holds. ◀

Now we conclude the proof of Theorem 15. Since ψ_{a+1} holds, we know that its body holds for the sets X_i defined as $X_i = \{j \mid \alpha(j) = i\}$, $i = 0, \ldots, a+1$ (Δ^0_1-comprehension is used here). Clearly these sets form a partition of $\mathbb{N}$ and thus the formula ψ_{a+1} gives us an index $i \leq a+1$ such that i is the maximal letter that appears infinitely many times in α. Since $\phi(0)$ holds we know that $i > 0$. If $i = a+1$ then by Claim 16 we obtain our thesis that $\phi(a)$ holds. Assume to the contrary that $i < a+1$. By Claim 16 it means that $\phi(i)$ and $\neg\phi(i+1)$ hold. This contradicts the assumption that $\forall i\, \big(\phi(i) \Rightarrow \phi(i+1)\big)$. Thus, a proof of $\phi(a)$ is concluded.

▶ Remark. The work of Sections 4–7 shows that the effectivity condition in Item 3. of Theorem 1 is not necessary to derive the other items in RCA_0. The bare statement that for every Büchi automaton there exists a complementing automaton already suffices.

The argument is as follows: assuming that each Büchi automaton can be complemented, the fixed-depth expressible property that a given word α does not satisfy the body of a

[4] $(n, k) \mapsto \frac{(n+k+1)(n+k)}{2} + k$ is one such map simple enough.

formula ψ_k as in (1) can be recognised by a Büchi automaton. By the proof of Lemma 14, if such an automaton accepts some infinite word, then it accepts an ultimately periodic infinite word. But this clearly shows that ψ_k is true for any k, thus proving Σ^0_2-IND and hence also the other items of Theorem 1.

8 Σ^0_2-IND implies Bounded-width König

$\mathsf{RCA}_0 + \Sigma^0_2$-IND is too weak to prove Weak König's Lemma (in fact, Σ^0_2-IND and WKL_0 are incomparable over RCA_0). However, it turns out that Σ^0_2-IND proves a restricted version of the lemma, where the "width" of the trees under consideration is globally bounded, in the sense that the subtree rooted in a vertex $\langle i_0, \ldots, i_\ell \rangle \in \{0, \ldots, k\}^*$ is completely determined by i_ℓ.

▶ **Theorem 17.** *Over RCA_0, Σ^0_2-IND implies Bounded-width König's Lemma (see Definition 3).*

Let us fix a graph G with vertices contained in $Q \times \mathbb{N}$ for some finite set Q. The usual way of proving König's Lemma starts by defining the subset G' of those vertices v of G for which the subgraph under v is infinite. Having defined G', we inductively pick any infinite path in G' and—assuming G does in fact contain arbitrarily long finite paths starting in $Q \times \{0\}$—we are guaranteed not to get stuck. The issue is whether we can obtain G' by Δ^0_1-comprehension.

A Π^0_1 definition of G' is provided by a standard trick used in the context of WKL_0. Notice that for every fixed n there can be at most $|Q|$ vertices of G of the form (q, n). Thus a vertex (q, n) is in G' if and only if it has the Π^0_1 property that for every $n' \geq n$ there exists a vertex (q', n') reachable from (q, n) by a path in G.

What remains is to give a Σ^0_1-definition of G'.

Consider two numbers $n < m$ and a vertex $v = (q, n)$ of G. We will say that v *dies before* m if there is no path in G from v that reaches a vertex of the form (q', m). For $i = 0, 1, \ldots, |Q|$ we will say that i *vertices die infinitely many times* if

$$\forall k\, \exists n > k\, \exists m > n. \text{ there are at least } i \text{ vertices of the form } (q, n) \text{ that die before } m.$$

Notice that the property of i that i *vertices die infinitely many times* is Π^0_2. Clearly if $i < i'$ and i' *vertices die infinitely many times* then i *vertices die infinitely many times*. By Σ^0_2-IND we can fix i_0 as the maximal i such that i *vertices die infinitely many times*. Notice that for each $i > i_0$ there exists $k(i)$ such that for every $m > n > k(i)$ there are fewer than i vertices of the form (q, n) that die before m. By Σ^0_2-collection, we can find a global bound k_0 such that $k_0 > k(i)$ for all $i > i_0$. This means that for $m > n > k_0$ we have at most i_0 vertices of the form (q, n) that die before m. Additionally, for infinitely many n there is $m > n$ such that exactly i_0 vertices of the form (q, n) die before m. The following claim shows how one can find a witness that the subgraph under a vertex v is infinite.

▶ **Claim 18.** *Assume that we are given $m > n > k_0$ and a vertex $v = (q, n)$ such that exactly i_0 vertices of the form (q', n) with $q' \neq q$ die before m. Then the subgraph under v is infinite.*

Proof. Assume to the contrary that for some $m' > m$ there is no vertex of the form (q', m') that can be reached from (q, n) by a path in G. It means that (q, n) dies before m'. Therefore, there are at least $i_0 + 1$ vertices of the form (q', n) that die before m'. This contradicts the way k_0 was chosen. ◀

Clearly, if for some $m > n$ and a vertex $v = (q, n)$ we know that v dies before m then the subgraph of G under v is finite.

We shall now use Claim 18 to give a Σ^0_1-definition of G'. We will say that $v = (q, n_0)$ belongs to G' if there exist $m > n > \max(k_0, n_0)$ and i_0 vertices of the form (q', n) such that all of them die before m and some other vertex of the form (q'', n) is reachable in G by a path from v. Clearly this is a Σ^0_1-definition. It remains to prove that it defines G'. First assume that v satisfies the above property and fix m, n, and (q'', n) as in the definition. By Claim 18 we know that the subgraph under (q'', n) is infinite. Since (q'', n) is reachable from v in G, this implies that also the subgraph under v is infinite and thus $v \in G'$. Now assume that $v = (q, n_0) \in G'$. By the choice of i_0 we know that there exist $m > n > \max(n_0, k_0)$ and exactly i_0 vertices of the form (q', n) that die before m. Since the subgraph under v is infinite, we know that some vertex of the form (p, m) is reachable from v in G. Notice that any path connecting v and (p, m) needs to contain a vertex of the form (q'', n). Clearly (q'', n) cannot be any of the i_0 vertices that die before m. Thus v satisfies the above condition.

▶ **Fact 19.** *If a vertex $(q, 0)$ of G satisfies the hypothesis of Bounded-width König's Lemma, then $(q, 0) \in G'$. Moreover, if $v = (q, n) \in G'$ then there exists $(q', n+1) \in G'$ such that there is an edge between (q, n) and $(q', n + 1)$.*

Now, given $(q, 0) \in G'$, we can construct an infinite path in G' using Δ^0_1-comprehension. Fix any linear order on Q. Let $\pi(0)$ be $(q, 0)$. If $\pi(n)$ is defined let $\pi(n + 1) = (q', n + 1)$ for the minimal $q' \in Q$ satisfying: $(q', n + 1) \in G'$ and there is an edge in G between $\pi(n)$ and $(q', n + 1)$. Fact 19 implies that π is well-defined. By the construction π is an infinite path in G' and thus in G.

9 Σ^0_2-IND implies determinisation

In this section we will show the following theorem.

▶ **Theorem 20.** *Over* RCA_0*,* Σ^0_2-IND *implies the existence of an algorithm which, given a nondeterministic Büchi automaton $\mathcal{B}$ over an alphabet Σ, outputs an equivalent deterministic Rabin automaton $\mathcal{A}$—the alphabet of $\mathcal{A}$ is Σ and for every infinite word α over Σ, $\mathcal{A}$ accepts α if and only if $\mathcal{B}$ accepts α.*

The proof scheme presented here is based on a determinisation procedure proposed in [13] (see [1, 8] for similar arguments and a comparison of this determinisation method to the method of Safra). Our exposition follows lecture notes of M. Bojańczyk [2]. Although the general structure of the argument is standard, we need to take additional care to ensure that the reasoning can be conducted in RCA_0 using only Σ^0_2-IND.

The proof of Theorem 20 will be split into separate steps that will allow us to successively simplify the objects under consideration. To merge these steps we will use the notion of a deterministic transducer that transforms one infinite word into another.

▶ **Definition 21.** A transducer is a deterministic finite automaton, without accepting states, where each transition is additionally labelled by a letter from some *output alphabet.* More formally, a transducer with an input alphabet Σ and an output alphabet Γ is a tuple $\mathcal{T} = \langle Q, q_\mathrm{I}, \delta\rangle$ where $q_\mathrm{I} \in Q$ is an initial state and $\delta\colon Q \times \Sigma \to \Gamma \times Q$.

A transducer naturally defines a function $\mathcal{T}\colon \Sigma^\mathbb{N} \to \Gamma^\mathbb{N}$. Formally, such a function is a third-order object and thus not available in second-order arithmetic. However, given a word α, we can use Δ^0_1-comprehension to obtain the unique infinite word produced by $\mathcal{T}$ on input α. Whenever we write $\mathcal{T}(\alpha)$, we have this word in mind.

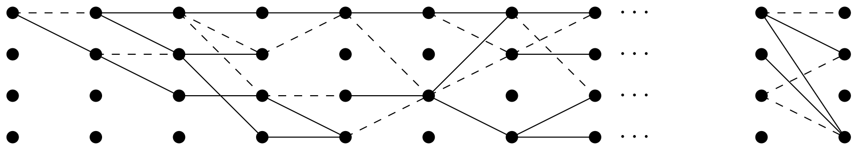

Figure 1 A Q-dag and a single letter from the alphabet $[Q]$. The accepting edges are represented by solid lines, and non-accepting edges are dashed lines.

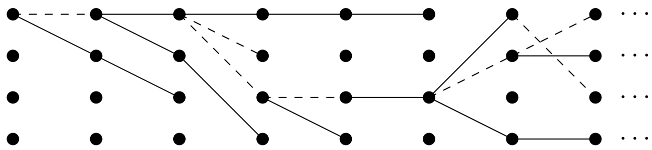

Figure 2 A tree-shaped Q-dag.

It is easy to see that a transducer can be used to reduce the question of acceptance from one deterministic automaton to another, as stated by the following lemma.

▶ **Lemma 22.** *For every deterministic Rabin automaton $\mathcal{A}$ with the input alphabet Γ, and every transducer $\mathcal{T}\colon \Sigma^{\mathbb{N}} \to \Gamma^{\mathbb{N}}$, there exists a deterministic Rabin automaton $\mathcal{A} \circ \mathcal{T}$ which accepts an infinite word $\alpha \in \Sigma^{\mathbb{N}}$ if and only if $\mathcal{A}$ accepts $\mathcal{T}(\alpha)$.*

One of the steps in the proof of Theorem 20, expressed by the lemma below, allows us to work with a fixed alphabet that depends only on the set of states of the given automaton $\mathcal{B}$. For that, we introduce a notion of a Q-dag. A Q-dag is an infinite word over the alphabet of transition matrices $[Q]$ of $\mathcal{B}$ that represents all the possible runs of $\mathcal{B}$ over a given infinite word, see Figure 1 (a formal definition will be given in the full paper).

▶ **Lemma 23.** *There exists a transducer $\mathcal{T}_1$ that inputs an infinite word $\alpha \in \Sigma^{\mathbb{N}}$ and outputs a Q-dag $\mathcal{T}_1(\alpha)$ such that $\mathcal{B}$ accepts α if and only if $\mathcal{T}_1(\alpha)$ contains an accepting path.*

This lemma is trivial—the transducer $\mathcal{T}_1$, after reading a finite word $w \in \Sigma^*$, stores in its state the set of states of $\mathcal{B}$ reachable from $q_{\mathrm{I}}^{\mathcal{B}}$ over w. The initial state of $\mathcal{T}_1$ is $\{q_{\mathrm{I}}\}$. Given a state $R \subseteq Q$ of $\mathcal{T}_1$ and a letter a, the transducer moves to the state

$$R' = \{q' \mid (q, a, q') \in \delta^{\mathcal{B}}\}$$

and outputs a letter $M \in [Q]$ such that $M(q, q') = M_a(q, q')$ if $q \in R$ and $M(q, q') = 0$ if $q \notin R$ (see Section 3 for the definition of M_a and $[Q]$). Clearly there is a computable bijection between the accepting runs of $\mathcal{B}$ over α and accepting paths in the Q-dag $\mathcal{T}_1(\alpha)$.

The next lemma shows that one can use a transducer to reduce general Q-dags to so-called *tree-shaped* Q-dags—the graph structure of such a word has the shape of a tree, see Figure 2.

▶ **Lemma 24.** *There exists a transducer $\mathcal{T}_2$ that inputs a Q-dag α' and outputs a tree-shaped Q-dag $\mathcal{T}_2(\alpha')$ such that α' contains an accepting path if and only if $\mathcal{T}_2(\alpha')$ contains an accepting path.*

To prove this lemma one uses a lexicographic order on paths in a given Q-dag. A crucial ingredient here is Bounded-width König's Lemma from Section 8. Additionally, we need to make sure that the graph to which Bounded-width König's Lemma is applied can be obtained using Δ^0_1-comprehension. For this purpose we use Σ^0_2-IND once again.

The proof of Theorem 20 is concluded by the following lemma and an application of Lemma 22.

▶ **Lemma 25.** *There exists a deterministic Rabin automaton $\mathcal{A}$ over the alphabet $[Q]$ that for every tree-shaped Q-dag $\alpha'' \in [Q]^{\mathbb{N}}$ accepts it if and only if α'' contains an accepting path.*

10 Conclusions and further work

In this work we have characterised the logical strength of Büchi's decidability theorem and related results over the theory RCA_0. We proved over RCA_0 that complementation for Büchi automata is equivalent to Σ^0_2-IND, as is the decidability of $\mathrm{MSO}(\mathbb{N}, \leq)$ (to the extent that this can be expressed).

Without Σ^0_2-IND, many aspects of automata on infinite words seem to make little sense (note, for instance, that the very concept of "a state occurs only finitely often" is Σ^0_2). The picture suggested by our work is that this minimal reasonability condition already suffices to prove all the basic results. This situation is completely different for automata on infinite trees, where the concepts also make sense already in $\mathsf{RCA}_0 + \Sigma^0_2$-$\mathsf{IND}$, but proving the complementation theorem or decidability of MSO requires much more [9].

We are thus led to the general question whether the entire theory of automata on infinite words requires exactly $\mathsf{RCA}_0 + \Sigma^0_2$-$\mathsf{IND}$. This includes in particular the following issues:

- Does McNaughton's determinisation theorem imply Σ^0_2-IND over RCA_0?
- How much axiomatic strength is needed to develop the algebraic approach to MSO ([14, Chapter II]), for instance to prove that Büchi-recognisability is equivalent to recognisability by finite Wilke algebras?
- What about developing the Wagner hierarchy (see [14, Chapter V.6])?
- Does $\mathsf{RCA}_0 + \Sigma^0_2$-$\mathsf{IND}$ prove the uniformisation theorem for automata, in the form: for a given automaton $\mathcal{A}$ over the alphabet $\{0,1\}^2$ such that $\forall X\, \exists Y\, (\mathcal{A}$ accepts $X \otimes Y)$, there exists an automaton $\mathcal{B}$ such that $\forall X\, \exists! Y$ (both $\mathcal{A}$ and $\mathcal{B}$ accept $X \otimes Y$) (see [15, Theorem 27])?

References

1 Christoph Schulte Althoff, Wolfgang Thomas, and Nico Wallmeier. Observations on determinization of Büchi automata. *Theor. Comput. Sci.*, 363(2):224–233, 2006. `doi:10.1016/j.tcs.2006.07.026`.

2 Mikołaj Bojańczyk. Lecture notes on languages, automata and computations, University of Warsaw, 2015. URL: `http://www.mimuw.edu.pl/~bojan/20152016-2/jezyki-automaty-i-obliczenia-2/mcnaughtons-theorem`.

3 J. Richard Büchi. On a decision method in restricted second order arithmetic. In Ernest Nagel, Patrick Suppes, and Alfred Tarski, editors, *Logic, Methodology and Philosophy of Science. Proceeding of the 1960 International Congress*, pages 1–11. Stanford University Press, 1962.

4 Petr Hájek and Pavel Pudlák. *Metamathematics of first-order arithmetic.* Perspectives in Mathematical Logic. Springer-Verlag, Berlin, 1993. `doi:10.1007/978-3-662-22156-3`.

5 Denis R. Hirschfeldt. *Slicing the truth*, volume 28 of *Lecture Notes Series. Institute for Mathematical Sciences. National University of Singapore.* World Scientific, 2015.

6 Jeffry L. Hirst. *Combinatorics in Subsystems of Second Order Arithmetic.* PhD thesis, Pennsylvania State University, 1987.

7 Carl G. Jockusch, Jr. Ramsey's theorem and recursion theory. *J. Symbolic Logic*, 37:268–280, 1972.

8 Detlef Kähler and Thomas Wilke. Complementation, disambiguation, and determinization of Büchi automata unified. In *ICALP*, pages 724–735, 2008. `doi:10.1007/978-3-540-70575-8_59`.

9 Leszek Aleksander Kołodziejczyk and Henryk Michalewski. How unprovable is Rabin's decidability theorem? (accepted@LICS 2016). *CoRR*, abs/1508.06780, 2015. URL: http://arxiv.org/abs/1508.06780.

10 G. Kreisel. A variant to Hilbert's theory of the foundations of arithmetic. *British J. Philos. Sci.*, 4:107–129, 1953.

11 Jiayi Liu. RT^2_2 does not imply WKL_0. *J. Symbolic Logic*, 77(2):609–620, 2012. doi:10.2178/jsl/1333566640.

12 Robert McNaughton. Testing and generating infinite sequences by a finite automaton. *Information and Control*, 9(5):521–530, 1966. doi:10.1016/S0019-9958(66)80013-X.

13 David E. Muller and Paul E. Schupp. Simulating alternating tree automata by nondeterministic automata: New results and new proofs of the theorems of Rabin, McNaughton and Safra. *Theoretical Computer Science*, 141(1–2):69–107, 1995. doi:10.1016/0304-3975(94)00214-4.

14 Dominique Perrin and Jean-Éric Pin. *Infinite words : automata, semigroups, logic and games*. Pure and Applied Mathematics. Elsevier, London, San Diego (Calif.), 2004.

15 Alexander Rabinovich. On decidability of monadic logic of order over the naturals extended by monadic predicates. *Information and Computation*, 205(6):870–889, 2007.

16 Saharon Shelah. The monadic theory of order. *Ann. of Math. (2)*, 102(3):379–419, 1975.

17 Stephen G. Simpson. *Subsystems of second order arithmetic*. Perspectives in Mathematical Logic. Springer-Verlag, Berlin, 1999. doi:10.1007/978-3-642-59971-2.